



**FOR IMMEDIATE RELEASE
FEBRUARY 16, 2000**

CONTACT: Mary Jane Collipriest, 202-224-5444, Washington, D.C. 20510

BENNETT ANNOUNCES HEARING ON FINANCIAL SERVICES AND ANALYSIS CENTER

Hearing will explore information-sharing to prevent cyber attacks

WASHINGTON, DC -- U.S. Senator Bob Bennett (R-Utah), Chairman of the Senate Banking Subcommittee on Financial Institutions, today said he plans to ask representatives of a banking industry computer security group why information was not shared with other businesses and federal officials that may have aided the investigation into recent attacks against prominent e-commerce web sites.

"Crimes in cyberspace demand more agile responses from businesses to protect themselves, and open lines of communication between law enforcement agencies and private sector businesses," said Bennett, whose study of the Y2K problem has highlighted high-tech vulnerabilities in U.S. critical infrastructures. "With this in mind, I am greatly troubled by the apparent inability of financial services companies to share information with other U.S. companies about the looming danger of material damage to their businesses."

At issue is a report that the Treasury Department prevented industry warnings from being passed on to other companies about the likely sources of last week's cyber attacks. Senator Bennett has scheduled a hearing in the Senate Banking Subcommittee on Financial Institutions, which will address questions regarding who possessed information about potential attackers, and what caused a delay in information from being passed to regulators and other hacking victims. Bennett also said he has questions about how severe an attack would have to be before private industry shared information; what is being done to combat cyber crime internationally, and what plans are in place to rebuild systems after they are hacked. The hearing will be held March 1 at 9:30 a.m. Eastern Time, location to be determined.

"It strikes me as reasonable that any corporate 'Good Samaritan' would act quickly to warn other members of the business community or law enforcement officials of the existence of malicious computer code whose sole purpose is launch a denial-of-service attack," said Bennett. "As with the year 2000 technology problem, the role of the federal government must be to remove impediments to company-to-company communication, and to facilitate a partnership for defending against Information Age attacks."

Bennett also said he is monitoring development of the National Plan, the Administration's blueprint for national critical infrastructure protection (CIP), which he will address during the National CIP Partnership Retreat, hosted by the U.S. Chamber of Commerce in Washington, D.C., on February 22.

"Rapid developments in information technology, and the implementation of new productivity-enhancing business systems have created severe information infrastructure risks in businesses both large and small," said Bennett. "It is critical that we develop a partnership allowing a beneficial flow of information for e-defense while preserving privacy and protecting America's competitive strongholds."

###

<http://www.senate.gov/~bennett>